PEO EIS

PEO ENTERPRISE INFORMATION SYSTEMS

TRANSPORTATION INFORMATION SYSTEMS

TRANSPORTATION INFORMATION SYSTEMS (TIS)

USER ACCOUNT MANAGEMENT GUIDE

10 MAY 2005

Table of Contents

TIS User Account Management Policy

I. Introduction

This document establishes the User Account Management process for the Transportation Information Systems (TIS) Enterprise. This process covers all aspects of the User Account Management construct, from the appointment of the User Account Manager (UAM) to the account creation process. Process models are provided in this document for the creation, deletion, and modification of TIS user accounts. These models apply to all of the applications hosted on the TIS Enterprise. Currently, this includes TC-AIMS II, TIS-TO, and AALPS.

The procedures defined in this policy relate specifically to Enterprise operations. User account management mechanisms are available in the breakaway configuration as well. The breakaway user account management processes are identified in a separate document.

Individuals involved in the User Account Management process are identified below:

Actors (Roles in User Account Management Processes)

- TIS User – End user of one or more of the TIS applications hosted at the TIS Enterprise.
- User Account Manager (UAM) – A trusted TIS agent at a local installation that has been granted the authority to authorize and facilitate the creation, maintenance, and overall management of TIS accounts and application profiles for a defined user population (e.g., for users belonging to a defined set of units/UICs).
- TIS Helpdesk – Consists of TIS Help Desk Tier I and II, as well as automated functionality to be implemented in Service Desk.
- Approval Authority – The commander of the Brigade or equivalent level specific military unit (or their official designee) that can appoint UAMs, authorize user access to a TIS application and to a unit's UICs and data within TIS applications.
- Security Officer – Appointed security officer at a local installation that can verify and maintain the background investigation/ADP level of individuals requesting access to the TIS Enterprise**.**

II. The User Account Manager (UAM)

Units throughout the Armed Forces must be prepared to deploy and fulfill their operational missions at all times. To successfully accomplish this task, units must have trained system operators to manipulate operational data and ensure deployment requirements are met. To de-centralize the TIS responsibility of establishing accounts for unit system users, the Unit Account Manager was created.

The Purpose of the UAM

The User Account Manager (UAM) serves as the primary point of contact for the creation and maintenance of TIS Enterprise accounts for the unit level users. The UAM is entrusted to perform the positive identification of all designated users and possesses administrative control of all subordinate unit UICs and access to unit data.

UAM Appointment

User Account Managers are required for all installations/organizations that utilize TIS Enterprise applications. User Account Managers are designated at Brigade (or equivalent) level units and organizations. To ensure proper operational coverage and redundancy, TIS JPMO recommends that at least two (but no more than three) UAMs be appointed for each Brigade. UAMs are appointed via UAM Appointment Memorandum (see Attachment 1). The appointment memorandum specifies the name, rank, SSN, AKO email address, and phone number of each UAM being appointed, as well as the list of UICs each UAM will be responsible for. The memorandum must be signed by the Brigade-level (O-6) commander equivalent (e.g. GS-15, etc). Navy UAMs must be appointed by an O-5 or their equivalent. Exceptions for the O-6 signature requirement will be reviewed on a case-by-case basis for Detachments and/or smaller organizations that do not correlate directly to a Brigade level command. For these cases, the highest level commander can act as the approval authority for the appointment of their UAMs. Upon completion, the UAM appointment will be sent to the TIS Helpdesk via FAX or email.

III. TIS User Account Creation

Once the UAM has been designated and appointed, they can begin to facilitate account creation for their unit(s). The TIS Enterprise User Account Creation process (detailed below) is followed to obtain a user account for Citrix and all applications (TC-AIMS II, AALPS, TIS-TO):

1. User downloads the TIS Enterprise Account Request Form (see Attachment 2) from the TIS Web Site (https://www.tis.army.mil). The form can be found in the Help Desk section.
2. In parallel with completion of the Account Request Form , the user requests that the Unit Security Manager produce and send a Visit Authorization Request (VAR) to the TIS Security Manager (for VAR example, see Attachment 4)
3. The UAM completes and signs the Account Request Form and sends it to the TIS Helpdesk via FAX (703-752-0737) or email (tishelpdesk@eis.army.mil).
4. The Unit Security Manager sends the completed VAR to the TIS Security Manager via FAX (703-752-0732) or email (steven.mcneil@eis.army.mil).
5. The TIS Helpdesk receives the account request, and verifies that the individual requesting the account has a current VAR on file with the TIS Security Manager.
6. Upon VAR verification, the TIS Helpdesk creates the user's Enterprise account(s). Account Requests that specify an upcoming ATRRS training course will have training and operational accounts created simultaneously. If a past ATRRS training course date is provided, or if the training information fields are left blank, only an operational account will be created. (NOTE: The Enterprise Account Request Form asks the user for their AKO or NMCI email address. This relates specifically to Army, Navy, and Marine Corps users. Providing this information is key to the account creation process. The intent of the TIS Enterprise Account Creation Process is to utilize the AKO/NMCI email alias as the user-id for the requested enterprise accounts.)
7. After the accounts have been created, the TIS Helpdesk will send the user-id and password information to the user's email address specified on the form. User-ids and

passwords will be sent in separate emails to ensure proper information security is maintained.

IV. UAM Account Creation

UAMs that request TIS Enterprise accounts must first be appointed in writing by their brigade or equivalent-level unit commander. TIS must have proof of this appointment on file, as well as a current VAR on file with the TIS Security Manager. The requesting UAM will initiate the request by completing an on-line form available via the TIS Web Site. A trusted individual within JPMO TIS will need to perform the positive identification. TIS will perform this identification by contacting the UAMs appointing commander to verify the need for access. Upon verification, the UAMs account request will be sent to the TIS Helpdesk for approval and signature. The UAMs userid and password information will be sent (separately) via email.

V. Account Maintenance

Under the Enterprise Account Creation construct, users require a mechanism to make changes to their Enterprise accounts. To facilitate this requirement, TIS has published the Enterprise Account Change Request Form (Attachment 3). This form will be downloaded from the TIS Web Site and completed by the Enterprise user requiring the account change. To ensure that the requested change is appropriate for the user, the UAM must sign the request. Upon completion, the Enterprise Account Maintenance Request Form will be sent to the TIS Helpdesk via fax or email. Listed below are the account maintenance options that TIS users will be able to request:

Add Access to Existing TIS User Account

This process would be used to grant Enterprise user with an existing TIS user account additional access to applications, UICs, and/or profiles. The requesting user will initiate the request by completing TIS Account Maintenance Form ICW UAM approval. TIS users may only request the addition of applications, UICs, and/or profiles to their own TIS account.

Change Access for an Existing TIS User Account

Under this process, access within a TIS Enterprise account (application, UIC, or profile) can be changed. This process can be used to exchange access within TIS applications, as well as making modifications and/or corrections to UICs and profiles. TIS Enterprise users will only be able to request changes to their own accounts. The TIS Enterprise user can initiate the deletion of an application from their account (and only from their account) by logging into the TIS portal and completing an on-line form available within the TIS portal. UAMs will also have the ability to initiate the deletion of an application from a TIS user account within their defined user community

Existing TIS User Account Access Elimination

This process is used to eliminate access to applications, UICs, and/or profiles for an existing TIS user account. The TIS Enterprise user initiates the request by completing TIS Account Change Request Form ICW UAM approval. To protect against accidental or

erroneous TIS application account deletions, the account will initially be disabled for a period of 15 days before access to it is permanently removed. TIS users may only request the removal of applications, UICs, and/or profiles to their own TIS account.

Reset User's TIS Portal Password

Password resets for all TIS Enterprise accounts are handled as requests to the TIS Helpdesk. These requests can be communicated to the TIS Helpdesk via telephone, fax, or email. Positive identification of the requesting individual is verified prior to password reset. The new password information will be sent to the individual's designated email account.

Delete TIS User Account

Deleting a TIS user account involves deleting the user's TIS portal (i.e., Citrix) account, as well as deleting all of the individual's application accounts (e.g., TC-AIMS II, TIS-TO, AALPS). The TIS end user can initiate the deletion of his own account (and only his own account) by completing the TIS Enterprise Account Change Request Form available via the TIS Web Site. UAMs may initiate the deletion of TIS user accounts within their defined user community. Bulk account deletions can be processed using the Change Request Form – an additional sheet specifying the users to be deleted must be included. To protect against accidental account deletions, the account will initially be disabled for a period of 15 days before it is permanently deleted.

VI. Enable/Disable TIS User Account

This process allows the TIS Enterprise user to disable or enable a TIS User Account ICW UAM approval. UAMs may initiate the disabling/enabling of TIS user accounts within their defined user community. Bulk account enabling/disabling can be processed using the Change Request Form – an additional sheet specifying the users to be enabled/disabled must be included.

VII. Contacting TIS

The TIS Helpdesk can be contacted in several ways:

Phone: 1-866-TCAIMS2 (1-866-822-4672)
(703)752-0806
(703)752-0888 ext 174

Please do not hesitate to contact us if you have any questions or concerns reference User Account Management.

TIS Web Site: https://www.tis.army.mil

[To be completed on Unit Letterhead] **[Date]**

[Unit Office Symbol]

MEMORANDUM FOR Joint Program Management Office, Program Manager, Transportation Information Systems, 8000 Corporate Court, Springfield, VA 22153

SUBJECT: Designation of TIS User Account Manager and Alternate User Account Manager

1. The undersigned designates and assigns the duties of TIS User Account Manager and Alternate User Account Manager to the following individuals. Designees will be responsible for submitting requests for and management of user accounts for the UICs listed here. This command takes full responsibility for any security incidents that may occur on the TIS Enterprise as a result of assigned individuals performing an untrustworthy act.

2. TIS User Account Manager _____(name, rank, SSN, duty title and office, contact email, and phone numbers)

3. TIS Alternate User Account Manager _____(name, rank, SSN, duty title and office, contact email, and phone numbers)

3. List of applicable UICs

_____
_____
_____

3. Point of contact at this headquarters is the undersigned. **[include POC phone number/email address]**

Signature Block
(Bde Level Unit Commander or equivalent)

Attachment: 1: UAM Appointment Memo

Attachment 2: TIS Enterprise Account Request Form

ENTERPRISE ACCOUNT REQUEST FORM
Transportation Information Systems

PART I *(To be completed by the User requesting access with UAM assistance. **NOTE**: An additional sheet specifying Name, SSN, AKO Address, Account Type, Application, UIC Access, Contact Information, and Profile can be used for bulk account registration.)*

1. Name *(Last, First, Middle)*: Grade/Rank:	*2.* Date:
3. Social Security Number:	*4.* Email Address (AKO or NMCI preferred):

5. Account Specification:

Training Information: ATRRS Course Number: Training Date:

Application Access: ☐ TC-AIMS II ☐ AALPS ☐ TIS-TO

UIC Access:

Profile(s): ☐ Company UMO ☐ Battalion UMC ☐ Brigade UMC ☐ ITO
☐ ITO Freight ☐ ITO Unit Move ☐ MCE ☐ Mode Operator
☐ Mode Manager ☐ TTP/MP Manager ☐ Enterprise Training ☐ Read-Only

6. Unit Name: Assigned UIC: Echelon:	*7.* Location (building #):
8. Phone (DSN): (Commercial):	*9.* Installation:
10. User Role(s):	*11.* GBLOC ID (ITO Users only): *12.* DODAAC ID:
13. Security Question: *What High School did you graduate from?*	*14.* UAM Name:
15. UAM Phone: (DSN): (Commercial):	*16.* UAM Email Address:

17. **STATEMENT OF ACCOUNTABILITY:** I understand my obligation to protect my password. I assume responsibility for the data and system to which I am granted access, in accordance with applicable policy and guidance. I will not exceed my authorized access, and will report changes in my need to know authorization, employment or duty status, or security status immediately to my designated User Account Manager (UAM).

Requestor's Signature: **X** _____ Date:

PART II *(To be completed by the Unit User Account Manager)*

ORGANIZATION UAM APPROVAL: I have reviewed this request and assure that the responsible individuals have correctly completed their respective parts and the nominee will use the account in an appropriate manner.

Organization UAM's Signature: **X** Date:

PART III *(To be completed by TIS Personnel)*

User Id:	VAR Verification Date:	Account Created By:

Attachment 3: TIS Enterprise Account Change Request Form

ENTERPRISE ACCOUNT CHANGE REQUEST
Transportation Information Systems

PART I *(To be completed by the User requesting access with UAM assistance. **NOTE**: An additional sheet specifying Name, SSN, AKO Address, desired account changes, and Contact Information can be used for bulk account maintenance.)*

1. Name *(Last, First, Middle)*: Grade/Rank:	*2.* Date:
3. User Id:	*4.* Email Address (AKO or NMCI only): (ako username)@us.army.mil

5. Account Maintenance :

Type of Account Maintenance:

☐ Add Access ☐ Change Access ☐ Remove Access

☐ Delete Account ☐ Disable Account ☐ Enable Account

NOTE: If you are requesting multiple actions on your account(s), please describe your requirements in the REMARKS section.

Type of Account: ☐ Training ☐ Operational (Production)

Application Access: ☐ TC-AIMS II ☐ AALPS ☐ TIS-TO

UIC Access:

Profile(s): ☐ Company UMO ☐ Battalion UMC ☐ Brigade UMC ☐ ITO

☐ ITO Freight ☐ ITO Unit Move ☐ MCE ☐ Mode Operator

☐ Mode Manager ☐ TTP/MP Manager ☐ Enterprise Training ☐ Read Only

REMARKS

REQUESTOR'S CONFIRMATION: I will abide by the user policy set forth in DoDI 8500.2, "Information Assurance (IS) Implementation", page 10, paragraphs 5.12.1 through 5.12.12. I will not exceed my authorized access, and will report changes in my "need to know" authorization, employment or duty status, or security status immediately to my designated User Account Manager (UAM).

Requestor's Signature: **X**_____ Date:

PART II *(To be completed by the Unit User Account Manager)*

ORGANIZATION UAM APPROVAL: I have reviewed this request and assure that the responsible individuals have correctly completed their respective parts and the nominee will use the account in an appropriate manner.

Organization UAM's Signature: **X**_____ Date:

PART III *(To be completed by TIS Personnel)*

Change Completion Date:	Change Completed By:

Attachment 4 Sample Visit Authorization Request (VAR)

[To be completed on Unit Letterhead] **[Date]**

[Unit Office Symbol}

MEMORANDUM FOR Joint Program Management Officer, Program Manager, Transportation Information Systems

SUBJECT: Background Investigation

1. References:

a. DoD 5200.2-R, January 1987, DoD Personnel Security Program
b. AR 25-2, 14 November 2003, Information Assurance
c. AR 380-67, Army Personnel Security Program

2. The following individuals work in an IT-III position using **(insert name of TIS application, i.e. TC-AIMS II).** An appropriate background investigation (NAC, NACI, or equivalent) has been conducted and favorably adjudicated or is in progress by the investigative authority identified. Request these individuals be granted access to **(name of TIS Application)** via the TIS, CMF:

NAME	GRADE	SSAN/ID#	TYPE/DATE OF INVESTIGATION	INVESTIGATIVE AUTHORITY
Capodicasa Sofia	U4	112054590	NAC Equivalent/01062001	OPM/Carbinari, Vicenzia
Fabien, Donavan	SPC	123456789	NAC/In Progress	CCF
Loya, Michael	GS-12	987654321	NACI/01022000	OPM
Degee, Helmut	UA-05	418-IT-4980	NAC/06052002	OPM

3. Point of contact at this headquarters is the undersigned. **[include phone number/email address]**

Signature Block
(Personnel/Field Security officer)

DEPARTMENT OF THE ARMY
OFFICE OF THE PROGRAM EXECUTIVE OFFICER
ENTERPRISE INFORMATION SYSTEMS
(PEO EIS)
Transportation Information Systems PMO
8000 CORPORATE COURT
SPRINGFIELD, VIRGINIA 22153

REPLY TO
THE ATTENTION OF

SFAE-PS-TC

MEMORANDUM FOR:

SUBJECT: User background investigative requirements for access to Transportation Information Systems (TIS) Applications Hosted on the TIS Central Management Facility (TIS, CMF)

1. In accordance with DoD 5200.2-R, AR 25-2, and AR 380-67 all personnel requesting access to an unclassified sensitive DoD information system must be subjected to a background investigation to establish a level of trustworthiness. For foreign nationals and local nationals the background investigation must be favorably adjudicated before access is granted to a DoD information system.

2. TIS applications (TC-AIMS II, TIS-TO etc.) are designated unclassified Sensitive information systems. The Information Technology (IT) Access Category for non privileged TIS application users is IT-III. Access category IT-III gives the user non-privileged access to one or more DoD information systems/applications. Users can receive, enter and/or modify information in an information system/application or database to which they are authorized access. Users have access only to that data/information and those applications/networks to which they are explicitly authorized or have a need-to-know and cannot alter those or other user's authorizations. Personnel requesting access to TIS applications via the TIS, CMF will be subjected to the appropriate personnel security investigation as defined in DoD 5200.2-R and AR25-2.

- DoD Civilians working in an IT-III position require a National Agency Check plus Written Inquiries (NACI).
- Military personnel working in an IT-III position require a National Agency Check (NAC).
- Contractor personnel working in an IT-III position require a National Agency Check (NAC).
- Non-U.S. Citizens** working in an IT-III position require a National Agency Check (NAC).

**The following extracts from DoD 5200.2-R and AR25-2 will apply to Non-U.S. citizen employees overseas:

DoD 5200.2-R, Chapter 3, paragraph C3.5.4:

C3.5.4. Non-U.S. citizen Employees Overseas**.** A non-U.S. citizen employed by DoD Components overseas, whose duties do not require access to classified information, shall be the subject of at least the following record checks, initiated by the appropriate Military Department investigative organization prior to employment. These checks and any additional investigation must be consistent with the policy and procedures governing locally hired employees under Status of Forces Agreements.

DoD Components assume responsibility for permitting access to DoD systems, information, material, and areas when an investigation conducted by the host country does not meet the investigative standards of this Regulation.

C3.5.4.1. Host government law enforcement and security agency checks at the city, state (province), and national level, whenever permissible by the laws of the host government; and
C3.5.4.2. DCII/JPAS
C3.5.4.3. FBI (where information exists indicating residence by the non-U.S. citizen in the United States for one year or more since age 18)
C3.5.4.4. CIA as appropriate

AR 25-2, Section V Personnel Security

4–14. Personnel security standards, paragraph 4-14 (3) *(a), (b), (c)*

(3) IT–III.
(a) Defined as personnel in IA positions (for example, normal users, power user on individual systems for configuration) with non-privileged level access to ISs and devices.
(b) A favorable review of local personnel, base and military, medical, and other security records, as appropriate.
(c) Initiation of a NACIC (for civilians) or NAC (for military and contractors), as appropriate or favorable review of SF85P and Supplemental Questionnaire.

3. All organizations requesting access to TIS applications on the TIS, Enterprise must submit documentation verifying that the appropriate investigations have been conducted and have been favorably adjudicated for each individual identified. Acceptable documentation will consist of a memorandum signed by the organization's Personnel Security Officer (enclosure 1) verifying that each individual identified has had the appropriate investigation conducted or is being conducted. The memorandum will be attached to a cover letter signed by the organizations commander (Field Grade Commander) concurring that the investigations were conducted and favorably adjudicated or are in progress (enclosure 2).

4. No user will be granted access* to TIS applications via the TIS Enterprise until the proper documentation has been received and validated by the TIS personnel security officer.

*Although U.S. civilian personnel, military personnel, and U.S. contractor personnel may be granted interim access while the investigation is in progress, Non-U.S. citizen employees will not be given interim access (the investigation must be favorably adjudicated).

5. Any questions concerning this memorandum should be directed to Mr. Steven McNeil, Personnel Security Officer for TIS, phone 757-703-0827, e-mail: steven.mcneil@eis.army.mil..

B. J. Price
Director, Technical Management Division
Joint Program Management Office, Transportation Information Systems